CLAIMS

I claim:

[c1] 1. A method in a computing system for confirming receipt of a ballot choice selected by a voter, comprising:

receiving a first confirmation message from a first party, the content of the first confirmation message confirming the identity of a ballot choice received for the voter by a vote collection authority; and

receiving a second confirmation message from a second party that is independent of the first party, the content of the second confirmation message independently confirming the identity of the ballot choice received for the voter by the vote collection authority.

[c2] 2. The method of claim 1, further comprising displaying the content of the first and second confirmation messages,

such that both the displayed first confirmation message and the displayed second confirmation message may be compared by the voter to expected vote confirmation messages for the ballot choice selected by the voter to determine whether a ballot choice other than the ballot choice selected by the voter has been received for the voter by the vote collection authority.

[c3] 3. The method of claim 1, further comprising:

combining the content of the first and second confirmation messages to obtain a combined confirmation message; and

displaying the combined confirmation message,

such that the displayed combined confirmation message may be compared by the voter to an expected combined vote confirmation message for the ballot choice selected by the voter to determine whether a ballot choice other than the ballot choice selected by the voter has been received for the voter by the vote collection authority.

[c4] 4. The method of claim 3 wherein the combined confirmation message is obtained using concatenating content from each of the first and second confirmation messages.

[c5] 5. The method of claim 3 wherein the combined confirmation message is obtained using a threshold secret reconstruction technique.

[c6] 6. The method of claim 1 wherein each of the first and second confirmation messages contains a value, and wherein the combined confirmation message is obtained by determining the product of the values contained in the first and second confirmation values.

[c7] 7. The method of claim 1 wherein each of the first and second confirmation messages contains a first value and a second value, wherein the combined confirmation message is obtained by:

determining the product of the first values contained in the first and second confirmation messages; and

determining the product of the second values contained in the first and second confirmation messages.

[c8] 8. The method of claim 1, further comprising receiving a third confirmation message from a third party that is independent of the first and second parties, the content of the third confirmation message independently confirming the identity of the ballot choice received for the voter by the vote collection authority.

[c9] 9. A computer-readable medium whose contents cause a computing system to confirm receipt of a ballot choice selected by a voter by:

receiving a first confirmation message from a first party, the content of the first confirmation message confirming the identity of a ballot choice received for the voter by a vote collection authority; and

receiving a second confirmation message from a second party that is independent of the first party, the content of the second confirmation message independently confirming the identity of the ballot choice received for the voter by the vote collection authority.

[c10] 10. A computing system for confirming receipt of a ballot choice selected by a voter, comprising:

a confirmation receipt subsystem that receives both a first confirmation message from a first party and a second confirmation message from a second party, the second party being distinct from the first party, the content of the first and second confirmation message each independently confirming the identity of a ballot choice received for the voter by a vote collection authority.

[c11] 11. A computer memory device under the control of a voter containing a data structure for confirming receipt of a ballot choice selected by a voter, comprising:

a first confirmation message received from a first party, the content of the first confirmation message confirming the identity of a ballot choice received for the voter by a vote collection authority; and

a second confirmation message received from a second party that is independent of the first party, the content of the second confirmation message independently confirming the identity of the ballot choice received for the voter by the vote collection authority.

[c12] 12. A method in a computing system for confirming receipt of a ballot choice selected by a voter, comprising:

sending to a first recipient via a first communications channel a confirmation dictionary for a first voter containing a list of ballot choice confirmation messages ordered in a first order; and

sending to the first recipient via a second communications channel that is distinct from the first communications channel a confirmation dictionary guide for the first voter indicating, for each of a plurality of valid ballot choices, a position in the first order containing a ballot choice confirmation message corresponding to the valid ballot choice,

such that the first recipient may use the identity of the ballot choice selected by the first voter together with the confirmation dictionary guide to identify in the confirmation dictionary the ballot choice confirmation message corresponding to the ballot choice selected by the voter.

[c13] 13. The method of claim 12 wherein the first recipient is the first voter.

[c14] 14. The method of claim 12, further comprising randomly selecting the first order.

[c15] 15. The method of claim 12, further comprising sending to a second recipient via the first communications channel a second confirmation dictionary for a second voter containing a list of ballot choice confirmation messages ordered in a second order, the second voter being distinct from the first voter, the second recipient being distinct from the first recipient, the second order being distinct from the first order.

[c16] 16. The method of claim 15 wherein the second recipient is the second voter.

[c17] 17. The method of claim 12 wherein the list of ballot choice confirmation messages contained in the confirmation dictionary includes a ballot choice confirmation message not corresponding to any valid ballot choice.

[c18] 18. The method of claim 12 wherein the list of ballot choice confirmation messages contained in the confirmation dictionary includes a distinguished plurality of ballot choice confirmation messages, none of the distinguished plurality of ballot choice confirmation messages corresponding to any valid ballot choice.

[c19] 19. The method of claim 12, further comprising:

receiving a ballot choice confirmation message corresponding to a ballot choice received for the voter at a ballot collection entity; and

displaying the received ballot choice confirmation message so that the recipient can compare the displayed ballot choice confirmation message with the ballot choice confirmation message identified in the confirmation dictionary as corresponding to the ballot choice selected by the voter.

[c20] 20. A computer-readable medium whose contents cause a computing system to confirm receipt of a ballot choice selected by a voter by:

sending to a recipient via a first communications channel a confirmation dictionary containing a list of ballot choice confirmation messages ordered in a first order; and

sending to the recipient via a second communications channel that is distinct from the first communications channel a confirmation dictionary guide indicating, for each of a plurality of valid ballot choices, a position in the first order containing a ballot choice confirmation message corresponding to that valid ballot choice,

such that the recipient may use the identity of the ballot choice selected by the voter together with the confirmation dictionary guide to identify in the confirmation dictionary the ballot choice confirmation message corresponding to the ballot choice selected by the voter.

[c21] 21. The computer-readable medium of claim 18, wherein the contents of the computer-readable medium further caused the computer system to:

receive a ballot choice confirmation message corresponding to a ballot choice received for the voter at a ballot collection entity; and

display the received ballot choice confirmation message so that the recipient can compare the displayed ballot choice confirmation message with the ballot choice confirmation message identified in the confirmation dictionary as corresponding to the ballot choice selected by the voter.

[c22] 22. A computing system for confirming receipt of a ballot choice selected by a voter, comprising:

a first transmission system coupled to a first communications channel that sends to a recipient a confirmation dictionary containing a list of ballot choice confirmation messages ordered in a first order; and

a second transmission system coupled to a second communications channel that is distinct from the first communications channel that sends to the recipient a confirmation dictionary guide indicating, for each of a plurality of valid ballot choices, a position in the first order containing a ballot choice confirmation message corresponding to the valid ballot choice,

such that the recipient may use the identity of the ballot choice selected by the voter together with the confirmation dictionary guide to identify in the confirmation dictionary the ballot choice confirmation message corresponding to the ballot choice selected by the voter.

[c23] 23. The computing system of claim 22 wherein the second transmission system sends the confirmation dictionary guide via a voice message.

[c24] 24. The computing system of claim 22 wherein the second transmission system sends the confirmation dictionary guide via a postal mail message.

[c25] 25. One or more generated data signals that collectively convey a randomized confirmation dictionary data structure, comprising a sequence of ballot confirmation strings, a subset of the ballot confirmation strings each corresponding to a different valid ballot choice, the order in which the ballot strings occur in the sequence being randomly selected, such that it cannot be determined without a separate confirmation dictionary guide which of the ballot confirmation strings in the sequence correspond to which valid ballot choices.

[c26] 26. The generated data signals of claim 25, wherein the ballot confirmation strings that correspond to valid ballot choices is a proper subset of the ballot confirmation strings in the sequence.

[c27] 27. A method in a computing system for delivering a ballot choice selected by a voter, comprising:

in a client computer system:

encrypting the ballot choice with a first secret known only to the client to generate a first encrypted ballot component;

encrypting the ballot choice with a second secret known only to the client, the second secret chosen independently of the first secret, to generate a second encrypted ballot component;

generating a proof demonstrating that the first and second encrypted ballot components are encrypted from the same ballot choice; and

sending the first and second ballot components and the proof to a vote collection computer system;

in the vote collection computer system:

determining whether the proof demonstrates that the first and second encrypted ballot components are encrypted from the same ballot choice; and

only if the proof demonstrates that the first and second encrypted ballot components are encrypted from the same ballot choice, accepting the ballot choice.

[c28] 28. The method of claim 27 wherein the first encrypted ballot component is generated by evaluating g^{α} and $h^{\alpha}m$, where p is prime; $g \in Z_p$, which has prime multiplicative order q, with the property that q is a multiplicity 1 divisor of $p-1$; $h \in \langle g \rangle$; $\alpha \in Z_q$ is chosen randomly at the voting node; and m is the ballot choice and wherein the second encrypted ballot component is generated by evaluating the expressions $g^{\bar{\alpha}}$ and $\bar{h}^{\bar{\alpha}}m$, where $\bar{h} \in \langle g \rangle$; $\bar{\alpha} \in Z_q$ is chosen randomly and independently at the voting node; and m is the ballot choice.

[c29] 29. The method of claim 27, further comprising:

in the vote collection computer system, sending to the client computer system a ballot confirmation based on the first and second encrypted ballot components; and

in the client computer system, decrypting the ballot confirmation using the first and second secrets.

[c30] 30. The method of claim 29, further comprising generating the ballot confirmation by evaluating the expression

$$V_i = K_i \overline{h}^{\beta_i(\alpha_i+\overline{\alpha}_i)} m^{(d+1)\beta_i}$$

Where p is prime; $g \in Z_p$, which has prime multiplicative order q, with the property that q is a multiplicity 1 divisor of $p - 1$; $h \in \langle g \rangle$; $\overline{h} \in$ is h raised to the power d which is maintained as a secret; $\alpha \in Z_q$ and $\overline{\alpha} \in Z_q$ are chosen randomly and independently at the voting node; $K_i \in \langle g \rangle$; $\beta_i \in Z_q$; and m is the ballot choice,
and by evaluating the expression

$$\overline{h}^{\beta_i}$$

— and wherein these two evaluated expressions are sent to the client computer system as the ballot confirmation.

[c31] 31. The method of claim 29 wherein the ballot confirmation is decrypted by evaluating

$$\frac{V_i}{(\overline{h}^{\beta_i})^{(\alpha_i+\overline{\alpha}_i)}}$$

where p is prime; $g \in Z_p$, which has prime multiplicative order q, with the property that q is a multiplicity 1 divisor of $p - 1$; $h \in \langle g \rangle$; $\overline{h} \in$ is h raised to the power d which is maintained as a secret; $\alpha \in Z_q$ and $\overline{\alpha} \in Z_q$ are chosen randomly and independently at the voting node; $K_i \in \langle g \rangle$; $\overline{\beta_i} \in Z_q$; and V_i is received as part of the ballot confirmation.

[c32] 32. A method in a computing system for transmitting a ballot choice selected by a voter, comprising:

encrypting the ballot choice with a first secret known only to the client to generate a first encrypted ballot component;

encrypting the ballot choice with a second secret known only to the client, the second secret chosen independently of the first secret, to generate a second encrypted ballot component;

generating a proof demonstrating that the first and second encrypted ballot components are encryptions of the same ballot choice; and

sending the first and second encrypted ballot components and the proof to a vote collection computer system.

[c33] 33. A computer-readable medium whose contents cause a computing system to submit a ballot choice selected by a voter by:

encrypting the ballot choice with a first secret known only to the client to generate a first encrypted ballot component;

encrypting the ballot choice with a second secret known only to the client, the second secret chosen independently of the first secret, to generate a second encrypted ballot component;

generating a proof demonstrating that the first and second encrypted ballot components are encryptions of the same ballot choice; and

sending the first and second ballot components and the proof to a vote collection computer system.

[c34] 34. One or more generated data signals together conveying an encrypted ballot data structure, comprising:

a first encrypted ballot choice encrypted with a first secret known only to a client computer system to generate a first encrypted ballot component,

a second encrypted ballot choice encrypted with a second secret known only to the client computer system, the second secret chosen independently of the first secret, and

a proof; and

such that the ballot represented by the encrypted ballot data structure may be counted only where the proof demonstrates that the first and second encrypted ballot choices are encryptions of the same ballot choice.

[c35] 30. A method in a computing system for receiving a ballot choice selected by a voter, comprising:

receiving from a client computer system:

a first encrypted ballot choice encrypted with a first secret known only to the client to generate a first encrypted ballot component,

a second encrypted ballot choice encrypted with a second secret known only to the client, the second secret chosen independently of the first secret, and

a proof; and

only where the proof demonstrates that the first and second encrypted ballot choices are encryptions of the same ballot choice, accepting the ballot choice.

[c36] 36. A computer-readable medium whose contents cause a computing system to receive a ballot choice selected by a voter by:

receiving from a client computer system:

a first encrypted ballot choice encrypted with a first secret known only to the client to generate a first encrypted ballot component,

a second encrypted ballot choice encrypted with a second secret known only to the client, the second secret chosen independently of the first secret, and

a proof; and

only where the proof demonstrates that the first and second encrypted ballot choices are encryptions of the same ballot choice, accepting the ballot choice.